

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
21. Mai 2004 (21.05.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/042592 A2

(51) Internationale Patentklassifikation⁷: G06F 15/76

(21) Internationales Aktenzeichen: PCT/DE2003/003692

(22) Internationales Anmeldedatum:
5. November 2003 (05.11.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 51 839.4 7. November 2002 (07.11.2002) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
US): ROBERT BOSCH GMBH [DE/DE]; Postfach 30 02
20, 70442 Stuttgart (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): SCHNEIDER, Klaus
[DE/DE]; Hanseatenstr. 22, 71640 Ludwigsurg (DE).

AUE, Axel [DE/DE]; Thomas-Mann-Strasse 28, 70825
Kornthal-Muenchingen (DE).

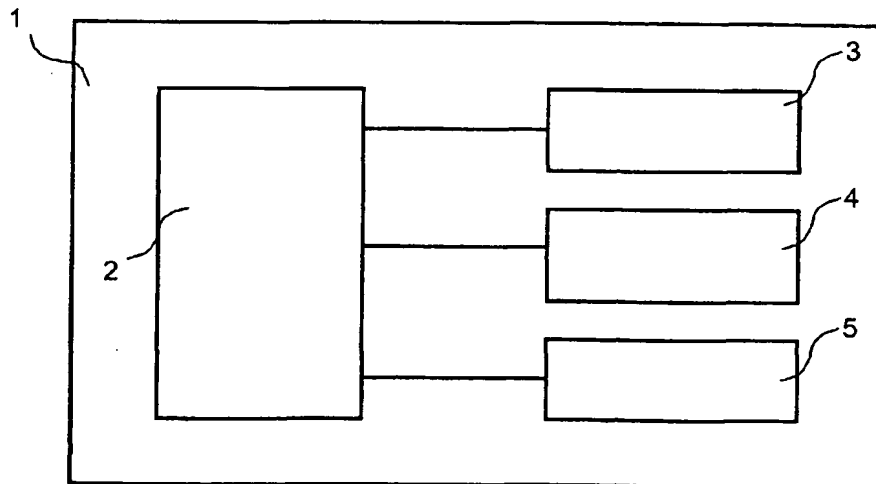
(81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR,
CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,
SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten (regional): ARIPO-Patent (BW,
GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU,
TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ,
DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC,
NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,
TG).

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR THE SECURE CHECKING OF A MEMORY REGION OF A MICROCONTROLLER IN A CON-
TROL DEVICE AND CONTROL DEVICE WITH A PROTECTED MIKROCONTROLLER

(54) Bezeichnung: VERFAHREN ZUR SICHEREN ÜBERPRÜFUNG EINES SPEICHERBEREICHES EINES MIKROCONT-
ROLLERS IN EINEM STEUERGERÄT UND STEUERGERÄT MIT EINEM GESCHÜTZTEN MIKROCONTROLLER



(57) Abstract: The invention relates to a method for operating a microcontroller in a control device in a motor vehicle with a central processor, at least one read-only memory region and at least one rewritable memory region, whereby at least one control programme is stored in the rewritable memory region, which is provided for processing by the central processor. According to the invention, a method for operation of a microcontroller in a control device, which better protects the checking of memories in the microcontroller against unpermitted access can be achieved, whereby a check programme is stored in a write-once memory region of the rewritable memory region and a service programme is stored in the read-only memory region. The check programme is called up at regular intervals by the control programme using the service programme and checks at least one part of the rewritable memory region. The service programme also restores a counter. The check programme, on a recognised manipulation of the checked memory region, or the counter, when the counter runs over, trip a RESET in the control device.

[Fortsetzung auf der nächsten Seite]

**Veröffentlicht:**

- ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Steuerung eines Mikrocontrollers in einem Steuergerät in einem Kraftfahrzeug mit einem Rechnerkern, wenigstens einem Nur-Lese-Speicherbereich und wenigstens einem wiederbeschreibbaren Speicherbereich, wobei in dem wiederbeschreibbaren Speicherbereich zumindest ein Steuerprogramm gespeichert ist, welches zur Verarbeitung durch den Rechnerkern vorgesehen ist. Um ein Verfahren zur Steuerung eines Mikrocontrollers in einem Steuergerät zu schaffen, welches die Überprüfung von Speichern des Mikrocontrollers besser gegen unerlaubte Eingriffe schützt, wird vorgeschlagen, ein Überprüfungsprogramm in einem einmal beschreibbaren Speicherbereich des wiederbeschreibbaren Speicherbereiches und ein Serviceprogramm im Nur-Lese-Speicherbereich zu speichern. Das Überprüfungsprogramm wird mittels des Serviceprogramms durch das Steuerprogramm in regelmäßigen Abständen aufgerufen und überprüft wenigstens einen Teil des wiederbeschreibbaren Speicherbereiches. Das Serviceprogramm setzt darüber hinaus einen Zähler zurück. Das Überprüfungsprogramm bei erkannter Manipulation des überprüften Speicherbereiches oder der Zähler bei Überlauf des Zählers lösen einen RESET des Steuergerätes aus.

5

Verfahren zur sicheren Überprüfung eines Speicherbereiches eines Mikrocontrollers in einem Steuergerät und Steuergerät mit einem geschützten Mikrocontroller

10

STAND DER TECHNIK

15

Die Erfindung betrifft ein Verfahren zur Steuerung eines Mikrocontrollers in einem Steuergerät in einem Kraftfahrzeug mit einem Rechnerkern, wenigstens einem Nur-Lese-Speicherbereich und wenigstens einem wiederbeschreibbaren Speicherbereich, wobei in dem wiederbeschreibbaren Speicherbereich zumindest ein Steuerprogramm gespeichert ist, welches zur Verarbeitung durch den Rechnerkern vorgesehen ist.

20

Weiterhin bezieht sich die Erfindung noch auf ein derartiges Steuergerät für ein Kraftfahrzeug mit einem Mikrocontroller.

25

Als Kraftfahrzeuge werden hier Fahrzeuge mit einer Brennkraftmaschine, welche mittels Steuergräten steuerbar ist, im weitesten Sinn verstanden. Derartige Steuergeräte werden in der Fahrzeugtechnik für vielfältige Funktionen verwendet, wie beispielsweise als Motorsteuergerät. Dabei wird zum Beispiel beim Chip-Tuning von Motorsteuergeräten häufig der nicht-flüchtige, aber mehrfach beschreibbare Speicher (z.B. Flash) manipuliert. Die dort gespeicherten Daten werden so verändert, dass eine höhere Motorleistung erreicht wird. Aus dem Stand der Technik sind auch Verfahren zur Steuerung der Mikrocontroller bekannt, die Überföhrungsroutinen beim Start und/oder während der Laufzeit des Steuergeräteprogramms aktivieren. Darüber hinaus wer-

35

den derartige Steuergeräte auch zur Steuerung von Getrieben oder ABS-Systemen eingesetzt.

- Aus der deutschen Offenlegungsschrift DE 197 53 730 ist ein
- 5 Verfahren und eine Vorrichtung zum Steuern einer Brennkraftmaschine bekannt. Die Vorrichtung umfasst wenigstens einen Mikroprozessor, wenigstens einen programmierbaren Speicher und einen wieder beschreibbaren Speicher. In dem wiederbeschreibbaren Speicher sind Programme und/oder Daten abgelegt, die vom
- 10 Mikroprozessor verarbeitet werden. Die Programme werden erst nach einer Prüfung abgearbeitet. Nimmt der Inhalt eines programmierbaren Speichers einen ersten Wert an, wird das Programm ohne weitere Prüfung abgearbeitet, anderenfalls erfolgt wenigstens eine weitere Prüfung. Mit diesem Verfahren soll er-
- 15 reicht werden, dass ein Datensatz, der veränderte Daten und/oder Programme enthält, oder der nicht vom Steuergerätehersteller freigegeben wurde, auf einem Seriensteuergerät lauffähig ist. Gleichzeitig soll der Kraftfahrzeughersteller die Möglichkeit haben, Steuergeräte zu applizieren, dass
- 20 heißt, Datensätze in einzelnen Steuergeräten zu verändern, ohne dass er Kenntnis von den Prüfungen hat. Problematisch ist hierbei der Schutz des Inhaltes des programmierbaren Speichers.
- 25 In der DE 197 23 332 A1 wird ein Verfahren zum Schutz eines Mikrorechners gegen Manipulation seines Programms und ein derart geschützter Mikrorechner beschrieben. Der Mikrorechner weist einen Rechnerkern, einen nur Lesespeicher und einen wiederbeschreibbaren Speicher auf. Im nur Lesespeicher ist ein
- 30 Überprüfungsprogramm gespeichert, das mittels eines Schlüssels aus dem Speicherinhalt des wiederbeschreibbaren Speichers ein Codewort bildet. Das Codewort wird dann mit einem Vergleichscodewort verglichen, das ebenfalls im wiederbeschreibbaren Speicher abgelegt ist. In Abhängigkeit von diesem Vergleich
- 35 wird der Mikrorechner gesperrt oder freigegeben.

Bei den bekannten Verfahren ist auch bei Verwendung eines geschützten, internen Flashbereich nur ein Schutz möglich, wenn die Anwendung nur diesen und keinen externen Speicher benötigt. Da die Anwendungen jedoch meist einen externen Speicher verwenden, wirkt der eingebaute Manipulationsschutz in diesen Anwendungen nicht - bzw. ist zu umgehen. Weiterhin ist eine Manipulation der Überprüfungsroutrinen dann möglich, wenn Controller ohne internen, geschützten Speicher eingesetzt werden. Im einfachsten Fall wird der Aufruf dieser Routinen verhindert.

Wenn dagegen diese Überprüfungsroutrinen in einem nicht änderbaren Bereich im Controller abgelegt werden (z.B. ROM), so bedeutet dies zum einen eine Kostensteigerung, zum anderen eine geringere Flexibilität in der Wahl der Algorithmen. Außerdem ist dabei auch oft ein ROM in der entsprechenden Controller-technologie nicht realisierbar. Selbst wenn ein ROM verfügbar ist, bleiben die Probleme, die grundsätzlich bei der Verwendung eines großen ROM-Bereiches zu beachten sind. Eine Änderung des Programmcodes ist sehr teuer, da jeweils neue Masken erforderlich sind. Wenn Code geändert werden muss, dauert es mindestens 4 Monate, bis der neue Code im Projekt einsetzbar ist (Liniendurchlaufzeit). Bei einem kundenspezifischen Code benötigt entweder jeder Kunde sein eigenes ROM, oder das ROM muss entsprechend vergrößert werden. Beides führt zu Mehrkosten, die nicht im Interesse des Kunden und des Halbleiterherstellers liegen. Auch hier ist ungelöst, wie die Ausführung des Codes erzwungen werden kann.

30

Die Problematik, die der vorliegenden Erfindung zugrunde liegt, besteht daher darin, ein Verfahren zur Überprüfung von Speichern eines Mikrocontrollers in einem Steuergerät zu schaffen, welches besser gegen unerlaubte Eingriffe schützt. Weiterhin besteht die Aufgabe darin, bei einem Mikrocontroller

35

in einem Steuergerät die unerlaubte Manipulation von Speicherinhalten wirkungsvoller zu verhindern.

VORTEILE DER ERFINDUNG

5

Das erfindungsgemäße Verfahren umfasst die folgenden Schritte: Speicherung eines Überprüfungsprogramms in einem einmal beschreibbaren Speicherbereich des wiederbeschreibbaren Speicherbereiches, Speicherung eines Serviceprogramms im Nur-Lese-Speicherbereich, Aufruf des Serviceprogramms durch das Steuerprogramm in regelmäßigen Abständen, Aufruf des Überprüfungsprogramms durch das Serviceprogramm, Rücksetzen eines Zählers durch das Serviceprogramm bei Aufruf durch das Steuerprogramm, Überprüfen wenigstens eines Teiles des wiederbeschreibbaren Speicherbereiches durch das Überprüfungsprogramm, Auslösen eines RESET durch das Überprüfungsprogramm bei Manipulation des überprüften Speicherbereiches oder durch den Zähler bei Überlauf des Zählers.

20 Das erfindungsgemäße Verfahren zeichnet sich dadurch aus, dass die Codesequenz zur Überprüfung des Speichers (das Überprüfungsprogramm) im nur einmal beschreibbaren Speicher nicht manipuliert werden kann. Ein solcher nur einmal beschreibbarer Speicherbereich kann zum Beispiel im vorhandenen, internen wiederbeschreibbaren Speicher (Flash) realisiert werden. Einige Mikrocontroller besitzen beispielsweise einen Passwortschutz auf Teile des internen Flash. Zum anderen wird beim Verfahren gemäß der Erfindung auch die Ausführung dieser Codesequenz wirkungsvoll sichergestellt. Im jeweiligen Steuerprogramm des Steuergerätes muss in regelmäßigen Abständen, die einstellbar sein können, ein Aufruf des Überprüfungsprogramms enthalten sein. Das Überprüfungsprogramm wird mittels eines Serviceprogramms aufgerufen, welches im Nur-Lese-Speicher gespeichert ist. Dieses Serviceprogramm ist somit vor unerlaubten Eingriffen und Manipulationen geschützt.

Dieses Serviceprogramm muss regelmäßig aufgerufen werden, da anderenfalls ein Zähler, der mittels einer Taktversorgung unbeeinflussbar, kontinuierlich läuft, einen Überlauf signalisiert. Der Zähler kann nicht angehalten werden, und nur durch den Aufruf des Serviceprogramms zurückgesetzt werden. Erreicht der Zähler vor dem Aufruf des Serviceprogramms einen Überlauf, erzeugt der Zähler einen RESET des Mikrocontrollers.

Der Zähler kann als separater Zählerbaustein mit einer eigenen Taktversorgung realisiert werden, der in einem geschützten Bereich innerhalb des Mikrocontrollers oder im Steuergerät angeordnet ist. Ebenso ist bei geeigneten Mikrocontrollern eine programmtechnische Implementierung denkbar. Der Überlauf des Zählers kann beispielsweise durch Erreichen des Zählerendes ausgelöst werden. Der Zeitpunkt des Erreichens des Überlaufes bestimmt den zeitlichen Abstand, nach dem das Serviceprogramm wieder aufgerufen werden muss, ohne dass der Zähler ein RESET auslöst. Zur Einstellung eines Zeitpunktes wird ein Zähler mit einem entsprechenden Zählerende gewählt oder ein Zählerstand eingestellt, der bei Erreichen ebenfalls ein Überlauf signalisiert. Bei Aufruf des Serviceprogramms durch das Steuerprogramm wird zum einen das Überprüfungsprogramm aufgerufen und zum anderen der Zähler zurückgesetzt.

Das RESET kann beispielsweise darin bestehen, dass das Steuergerät abgeschaltet wird oder mit einem Datensatz betrieben wird, der noch eine eingeschränkte Funktion erlaubt. Dabei kann auch gleichzeitig noch ein entsprechendes Signal an andere Steuergeräte abgegeben werden. Insbesondere ist es sinnvoll, ein Warnsignal auszugeben, welches eine Aufforderung zur Reparatur des Fahrzeuges in einer Werkstatt auslöst.

Des weiteren wird die Aufgabe der Erfindung noch durch ein Steuergerät für ein Kraftfahrzeug mit einem Mikrocontroller

gelöst, bei dem ein einmal beschreibbarer Speicherbereich des wiederbeschreibbaren Speicherbereiches zur Speicherung eines Überprüfungsprogramms vorgesehen ist, der Nur-Lese-Speicherbereich zur Speicherung eines Serviceprogramms vorgesehen ist, der Rechnerkern in regelmäßigen Abständen das Serviceprogramm nach Aufruf durch das Steuerprogramm verarbeitet, der Rechnerkern das Überprüfungsprogramm nach Aufruf durch das Serviceprogramm verarbeitet, ein Zähler vorgesehen ist, der durch das Serviceprogramm bei Aufruf durch das Steuerprogramm rücksetzbar ist, wenigstens ein Teil des wiederbeschreibbaren Speicherbereiches durch das Überprüfungsprogramm überprüfbar ist, ein RESET durch das Überprüfungsprogramm bei Manipulation des überprüften Speicherbereiches oder bei Überlauf des Zählers auslösbar ist.

Besonders bevorzugte Ausgestaltungen der Erfindung sind auch noch in den abhängigen Ansprüchen angegeben.

ZEICHNUNGEN

Im folgenden wird ein Ausführungsbeispiel der Erfindung anhand von zwei Zeichnungen näher erläutert. Dabei zeigen

Figur 1: ein Blockdiagramm eines erfindungsgemäßen Mikrocontrollers für ein Steuergerät und

Figur 2: ein Ablaufdiagramm des erfindungsgemäßen Verfahrens.

BESCHREIBUNG DER AUSFÜHRUNGSBEISPIELE

In der Figur 1 ist ein Mikrocontroller 1 für ein Steuergerät gemäß der Erfindung dargestellt. Er umfasst einen Rechnerkern 2, einen Nur-Lese-Speicher 3, einen nur einmal beschreibbaren Speicher 4 und einen wiederbeschreibbaren Speicher 5. Das Steuergerät kann beispielsweise ein Motorsteuergerät zur Steu-

erung von Drosselklappe, einzuspritzender Kraftstoffmenge oder anderer Größen sein. Aber auch ein Steuergerät zur Steuerung eines Getriebes, ABS-Systems oder anderer Systeme im Kraftfahrzeug ist ohne weiteres denkbar. Der Rechnerkern 1 ist ein
5 üblicher Mikroprozessor zur Verarbeitung der gespeicherten Programme und Daten. Der Nur-Lese-Speicher oder ROM (Read Only Memory) 3 enthält ein fest gespeichertes Programm, welches nur durch Austausch des ROM 3 geändert werden kann. In diesem Speicher ist in der Regel ein Minimalprogramm abgelegt, welches den Rechnerkern 1 in die Lage versetzt, Programme und Da-
10 ten aus den weiteren Speichern zu verarbeiten.

Der wiederbeschreibbare Speicher 5 ist meist als EPROM oder Flash-EPROM ausgeführt und enthält veränderbare Programme und
15 Daten des Steuergerätes. Der nur einmal beschreibbare Speicher 4 ist ein Speicherbereich des wiederbeschreibbaren Speichers 5 (Flash), der durch ein Passwort geschützt ist. In diesem Speicherbereich 4 ist eine Codesequenz gespeichert, welche die Aufgabe hat, die Code- und Datenbereiche des Mikrocontrollers
20 1 zu überprüfen. Dieses Überprüfungsprogramm ergreift bei erkannter Manipulation eine Gegenmaßnahme, die meist im Auslösen eines RESET besteht. Dabei kann das Ausmaß des RESET an die jeweils gewünschte Gegenmaßnahme angepasst werden. Das Steuergerät kann beispielsweise komplett abgeschaltet werden, was
25 bei einem Motorsteuergerät zu einem sofortigen Stillstand des Fahrzeuges führt. Oder das Steuergerät kann mit einer Minimal-konfiguration versorgt werden, so dass das Steuergerät funktionsbereit bleibt, jedoch zu einer vollständigen Funktionsfähigkeit eine Reparatur in einer Werkstatt erforderlich ist.

30 Die verschiedenen Speicherbereiche sind in der Figur 1 getrennt gezeichnet, wodurch jedoch nur ihre unterschiedliche Funktion gekennzeichnet werden soll. Es ist unter Wahrung der unterschiedlichen Funktionalität möglich, die Speicherbereiche
35 durch getrennte Bausteine oder in gemeinsamen Bausteinen zu

realisieren. So kann insbesondere der Flash-Speicher 5 sowohl innerhalb des Mikrocontrollerbausteins realisiert sein, als auch als externer Speicherbaustein.

5 In der Figur 2 ist der Ablauf des Verfahrens gemäß der Erfindung schematisch dargestellt. Die Bereiche A, B, C und D kennzeichnen die funktionell unterschiedlichen Speicherbereiche, in denen die jeweiligen Programme und Daten abgelegt sind. Im dargestellten Ausführungsbeispiel beschreibt A einen Hardware-
10 bereich im Mikrocontroller, B einen ROM-Bereich im Mikrocontroller und C einen Flash-Bereich im Mikrocontroller, während D einen externen Flash-Speicherbereich darstellt.

Im externen Flash D ist als Anwendungscode ein Steuerprogramm
15 für das Steuergerät gespeichert. Das Programm enthält im Code einen ,CALL'-Befehl, mit dem ein Serviceprogramm aufgerufen wird, welches im ROM-Speicherbereich B des Mikrocontrollers abgelegt ist. Bei einem entsprechenden Entry-Code wird ein ,SERVICE' im Serviceprogramm ausgelöst. Dieses Serviceprogramm
20 löst zwei Dinge aus, zum einen wird ein Zähler ,COUNTER' zurückgesetzt, der als Zählerbaustein im Mikrocontroller A realisiert ist. Der Zählerbaustein ist mit einer Taktleitung verbunden, so dass er unabhängig kontinuierlich läuft. Bei Erreichen eines maximalen Zählerstandes wird ein Überlauf signalisiert. Zum anderen wird gleichzeitig ein Sprung ,JUMP' in ein
25 Überprüfungsprogramm ausgelöst. Dieses Überprüfungsprogramm ist als Codesequenz im nur einmal beschreibbaren Speicherbereich im internen Flash gespeichert. Der interne Flash des Mikrocontrollers besitzt dazu einen Bereich, welcher durch ein
30 Passwort geschützt und damit nur einmal beschreibbar ist.

Das Überprüfungsprogramm überprüft mindestens einen Teil des vom Mikrocontroller verwendeten Speichers mittels bekannter Prüfmethoden, wie beispielsweise Checksummenbildung. Wenn an-
35 hand der Überprüfung eine Manipulation an den gespeicherten

Daten und / oder Programmen festgestellt wird, wird ein RESET ausgelöst. Wenn keine unerlaubte Veränderung festgestellt wird, wird mittels eines ,RETURN'-Befehls wieder zum Steuerprogramm zurückgekehrt.

5

Wenn der Zähler einen Überlauf signalisiert, dass heißt eine definierte Zeit abgelaufen ist, wird ebenfalls ein RESET ausgelöst. Dieses RESET kann wahlweise bedeuten, dass das Steuergerät komplett abgeschaltet wird oder das Steuergerät unter

10

Verwendung von vorher definierten Parametern betrieben wird. Dabei handelt es sich um eine Minimalkonfiguration, die eine Funktionalität des Steuergerätes noch gewährleistet, aber eine Reparatur in einer Werkstatt umgehend erforderlich macht. Der RESET bleibt so lange aktiv, bis das Gerät aus- und wieder

15

eingeschaltet wird (sogenannter Power-On RESET).

Da der Zähler unbeeinflusst kontinuierlich läuft, kann das Erreichen des Überlaufes und das damit zwingend verbundene RESET des Steuergerätes nur verhindert werden, wenn der Zähler re-

20

gelmäßig zurückgesetzt wird. Da dies nur vom Serviceprogramm im ebenfalls nicht manipulierbaren ROM-Bereich B ausgelöst werden kann, muss wiederum das Serviceprogramm regelmäßig vom Steuerprogramm aufgerufen werden. Daher kann das Steuerprogramm, welches den ,CALL'-Befehl enthalten muss, im relativ

25

ungeschützten Flash-Bereich D gespeichert sein. Denn auch durch Manipulationen kann folglich mit diesem Verfahren eine Überprüfung des Speichers des Mikrocontrollers nicht verhindert werden. Nur bei nicht manipulierten Speichern des Mikrocontrollers ist eine dauerhafte Funktionalität des Steuergerä-

30

tes gewährleistet.

Das erfindungsgemäße Verfahren bietet gegenüber bekannten Verfahren einige Vorteile. So entstehen nur sehr geringe oder keine Mehrkosten für den Controller-Chip, da nur ein minimaler Mehraufwand notwendig ist. Weiterhin kann das Überprüfungspro-

35

gramm individuell an Anforderungen oder Bedürfnisse angepasst werden, da diese Codesequenz nicht in der ROM-Maske enthalten ist. Somit kann es auch kundenspezifisch gehalten werden. Darüber hinaus kann der Controllerhersteller diese Funktionalität
5 auch anderen Kunden anbieten.

Es kann für Systeme ohne Controller-internes Flash das gleiche Verfahren angewendet werden. Dieses Verfahren behebt somit den Nachteil des geringeren Schutzes für Systeme mit internem und
10 externem Flash und ist in Kombination mit einer Paarung von Bauelementen ein sehr sicheres Verfahren. Obwohl der wiederbeschreibbare Speicherbereich beim obigen Ausführungsbeispiel innerhalb des Mikrocontrollers liegt, kann er selbstverständlich auch außerhalb liegen.

15

5

BEZUGSZEICHENLISTE:

1	Mikrocontroller
2	Rechnerkern
3	Nur-Lese-Speicherbereich
4	beschreibbarer Speicherbereich
5	wiederbeschreibbarer Speicherbereich

10

PATENTANSPRÜCHE

5

1. Verfahren zur Steuerung eines Mikrocontrollers (1) in einem Steuergerät in einem Kraftfahrzeug mit einem Rechnerkern (2), wenigstens einem Nur-Lese-Speicherbereich (3) und wenigstens einem wiederbeschreibbaren Speicherbereich (5), wobei in dem
- 10 wiederbeschreibbaren Speicherbereich (5) zumindest ein Steuerprogramm gespeichert ist, welches zur Verarbeitung durch den Rechnerkern (2) vorgesehen ist, umfassend mindestens die Schritte,
- Speicherung eines Überprüfungsprogramms in einem einmal beschreibbaren Speicherbereich (4) des wiederbeschreibbaren
 - 15 Speicherbereiches (5),
 - Speicherung eines Serviceprogramms im Nur-Lese-Speicherbereich (3),
 - Aufruf des Serviceprogramms durch das Steuerprogramm in regelmäßigen Abständen,
 - 20 - Aufruf des Überprüfungsprogramms durch das Serviceprogramm,
 - Rücksetzen eines Zählers durch das Serviceprogramm bei Aufruf durch das Steuerprogramm,
 - Überprüfen wenigstens eines Teiles des wiederbeschreibbaren Speicherbereiches durch das Überprüfungsprogramm,
 - 25 - Auslösen eines RESET durch das Überprüfungsprogramm bei Manipulation des überprüften Speicherbereiches oder durch den Zähler bei Überlauf des Zählers.
- 30 2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Steuerprogramm in einem internen Speicherbereich des Mikrocontrollers (1) gespeichert wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Steuerprogramm in einem externen Speicherbereich außerhalb des Mikrocontrollers (1) gespeichert wird.

5 4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Überprüfungsprogramm in einem internen Speicherbereich des Mikrocontrollers (1) gespeichert wird.

10 5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass das Überprüfungsprogramm in einem internen Speicherbereich des Mikrocontrollers (1) gespeichert wird, welcher durch ein Passwort geschützt ist.

15 6. Steuergerät für ein Kraftfahrzeug mit einem Mikrocontroller (1) mit einem Rechnerkern (2), wenigstens einem Nur-Lese-Speicherbereich (3) und wenigstens einem wiederbeschreibbaren Speicherbereich (5), wobei in dem wiederbeschreibbaren Speicherbereich (5) zumindest ein Steuerprogramm gespeichert ist, welches zur Verarbeitung durch den Rechnerkern (2) vorgesehen ist, wobei

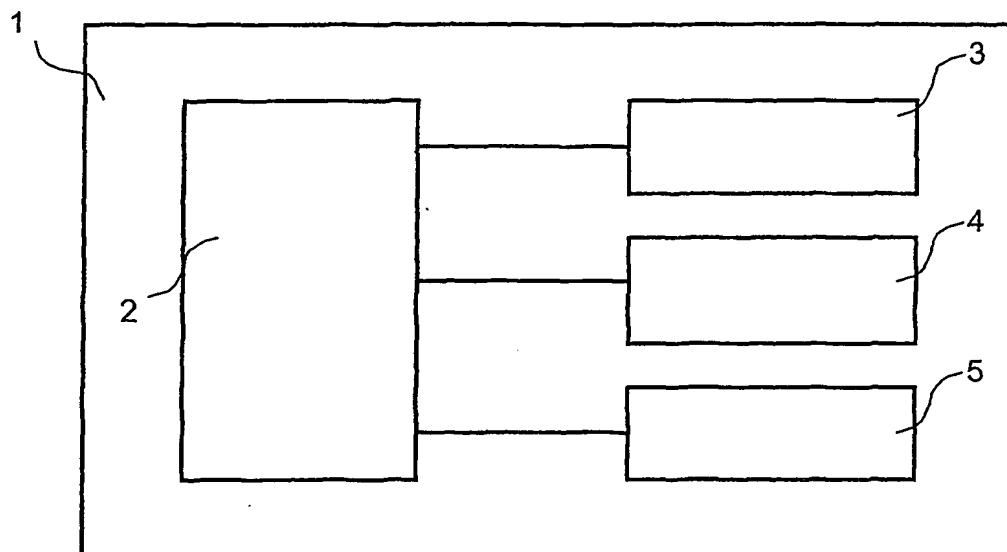
- ein einmal beschreibbarer Speicherbereich (4) des wiederbeschreibbaren Speicherbereiches (5) zur Speicherung eines Überprüfungsprogramms vorgesehen ist,
- der Nur-Lese-Speicherbereich (3) zur Speicherung eines Serviceprogramms vorgesehen ist,
- der Rechnerkern (2) das Serviceprogramm nach Aufruf durch das Steuerprogramm in regelmäßigen Abständen verarbeitet,
- der Rechnerkern (2) das Überprüfungsprogramm nach Aufruf durch das Serviceprogramm verarbeitet,
- 30 - ein Zähler vorgesehen ist, der durch das Serviceprogramm bei Aufruf durch das Steuerprogramm rücksetzbar ist,
- wenigstens ein Teil des wiederbeschreibbaren Speicherbereiches (5) durch das Überprüfungsprogramm überprüfbar ist,

- ein RESET durch das Überprüfungsprogramm bei Manipulation des überprüften Speicherbereiches oder bei Überlauf des Zählers auslösbar ist.

5 7. Steuergerät nach Anspruch 6, dadurch gekennzeichnet, dass der einmal beschreibbare Speicherbereich (4) innerhalb des Mikrocontrollers (1) angeordnet ist.

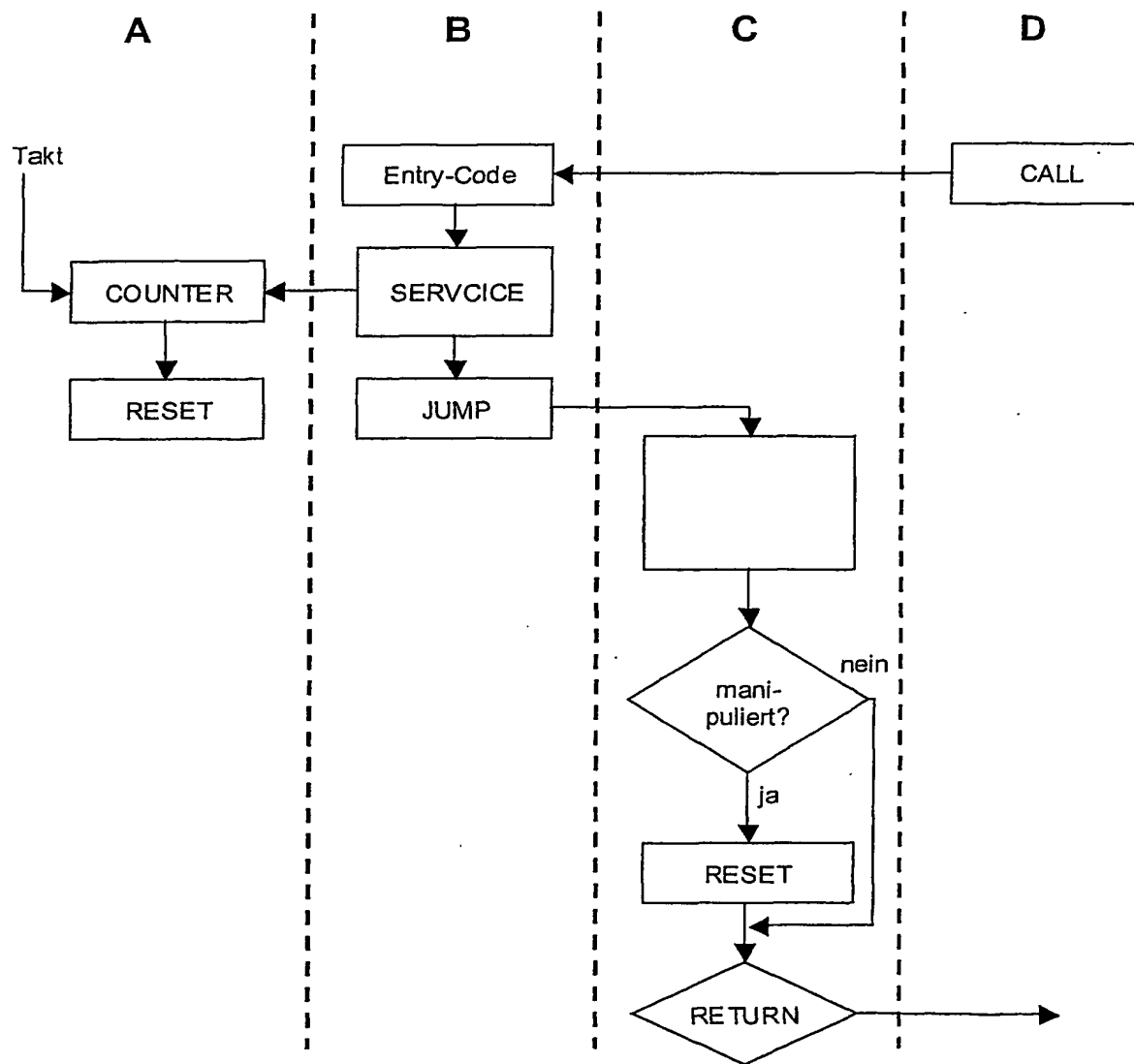
10 8. Steuergerät nach Anspruch 6, dadurch gekennzeichnet, dass der wiederbeschreibbare Speicherbereich (5) als Flash-Speicher ausgebildet ist.

1/2



FIGUR 1

2/2



Figur 2